

So senden Sie eine Beispielnachricht, um sicherzustellen, dass die Anti-Virus-Engine die Prüfung auf einer Cisco E-Mail Security Appliance (ESA) durchführt

Inhalt

[Einführung](#)

[So senden Sie eine Beispielnachricht, um sicherzustellen, dass die Anti-Virus-Engine die Prüfung auf einer Cisco E-Mail Security Appliance \(ESA\) durchführt](#)

[TXT-Datei erstellen](#)

[Senden einer Beispielnachricht](#)

[UNIX-CLI](#)

[Outlook](#)

[Überprüfung](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird beschrieben, wie Sie eine Beispielnachricht senden, um sicherzustellen, dass die Sophos-Antivirus- oder McAfee-Antivirus-Engine eine Prüfung auf einer Cisco Email Security Appliance (ESA) durchführt.

So senden Sie eine Beispielnachricht, um sicherzustellen, dass die Anti-Virus-Engine die Prüfung auf einer Cisco E-Mail Security Appliance (ESA) durchführt

Durch Senden einer Beispielnachricht mit einer viralen Testnutzlast über die ESA können wir die Sophos- oder McAfee-Antivirus-Engine auslösen. Bevor Sie die in diesem Dokument aufgeführten Schritte durchführen, müssen Sie Ihre Mail-Policy für eingehende oder ausgehende Nachrichten einrichten und die Mail-Richtlinie so konfigurieren, dass mit dem Virenschutz infizierte Nachrichten verworfen oder unter Quarantäne gestellt werden. Dieses Dokument verwendet ASCII-Code aus dem EICAR (www.eicar.org), der einen [Testvirus](#) als Anlage simuliert:

```
X50!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Hinweis: PRO EICAR: Diese Testdatei wurde der EICAR zur Distribution als "EICAR Standard Anti-Virus Test File" zur Verfügung gestellt und erfüllt alle oben aufgeführten Kriterien. Es ist sicher, sich weiterzugeben, weil es kein Virus ist, und enthält keine Fragmente von viralem Code. Die meisten Produkte reagieren darauf, als ob es sich um einen Virus handele (obwohl sie ihn in der Regel mit einem offensichtlichen Namen wie "EICAR-AV-Test" melden).

TXT-Datei erstellen

Erstellen Sie mit der ASCII-Zeichenfolge oben eine TXT-Datei, und legen Sie die Zeichenfolge so fest, wie sie als Text der Datei geschrieben wurde. Sie können diese Datei als Anlage in Ihrer Beispielnachricht senden.

Senden einer Beispielnachricht

Je nach Arbeitsweise können Sie die Beispielnachricht auf verschiedene Weise über die ESA senden. Zwei Beispielmethode werden über die UNIX-CLI mit der **E-Mail** oder über Outlook (oder eine andere E-Mail-Anwendung) verwendet.

UNIX-CLI

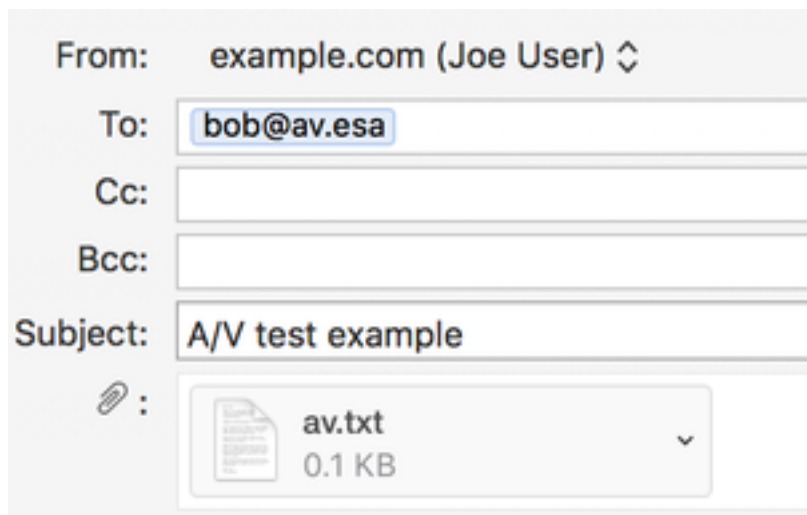
```
joe@unix.local:~$ echo "TEST MESSAGE w/ ATTACHMENT" | mail -s "A/V test example" -A av.txt bob@av.esa
```

Ihre UNIX-Umgebung muss korrekt eingerichtet sein, um E-Mails über die ESA zu senden oder weiterzuleiten.

Outlook

Bei Verwendung von Outlook (oder einer anderen E-Mail-Anwendung) haben Sie zwei Möglichkeiten, den ASCII-Code über folgende Kanäle zu senden: 1) mit der erstellten TXT-Datei, 2) direkter Einfügen der ASCII-Zeichenfolge in den Text der E-Mail-Nachricht.

Verwenden der TXT-Datei als Anlage:



The screenshot shows an Outlook email composition window. The 'From' field is 'example.com (Joe User)'. The 'To' field is 'bob@av.esa'. The 'Cc' and 'Bcc' fields are empty. The 'Subject' field is 'A/V test example'. Below the subject field, there is an attachment icon (a paperclip) and a list of attachments. The first attachment is 'av.txt' with a size of '0.1 KB' and a dropdown arrow to its right.

TEST MESSAGE w/ ATTACHMENT

Verwenden der ASCII-Zeichenfolge im Text der E-Mail-Nachricht:

From: example.com (Joe User) ↕
To: bob@av.esa
Cc:
Bcc:
Subject: A/V test example

X5O!P%@AP[4\PZX54(P^)7CC)7}\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H*

Ihr Outlook (oder eine andere E-Mail-Anwendung) muss korrekt eingerichtet sein, um E-Mails über Ihre ESA zu senden oder weiterzuleiten.

Überprüfung

Verwenden Sie auf der ESA-CLI den Befehl **tail mail_logs**, bevor Sie die Beispielnachricht senden. Beim Betrachten des E-Mail-Protokolls wird die Nachricht von McAfee als "VIRAL" gescannt und abgefangen:

```
Wed Sep 13 11:42:38 2017 Info: New SMTP ICID 306 interface Management (10.1.2.84) address 10.1.2.85 reverse dns host zane.local verified yes
Wed Sep 13 11:42:38 2017 Info: ICID 306 ACCEPT SG UNKNOWNLIST match sbrs[none] SBRS None country Australia
Wed Sep 13 11:42:38 2017 Info: Start MID 405 ICID 306
Wed Sep 13 11:42:38 2017 Info: MID 405 ICID 306 From: <joe@example.com>
Wed Sep 13 11:42:38 2017 Info: MID 405 ICID 306 RID 0 To: <bob@av.esa>
Wed Sep 13 11:42:38 2017 Info: MID 405 Message-ID '<20170913153801.0EDA1A0121@example.com>'
Wed Sep 13 11:42:38 2017 Info: MID 405 Subject 'A/V test attachment'
Wed Sep 13 11:42:38 2017 Info: MID 405 ready 1057 bytes from <joe@example.com>
Wed Sep 13 11:42:38 2017 Info: MID 405 attachment 'av.txt'
Wed Sep 13 11:42:38 2017 Info: ICID 306 close
Wed Sep 13 11:42:38 2017 Info: MID 405 matched all recipients for per-recipient policy my_av in the inbound table
Wed Sep 13 11:42:38 2017 Info: MID 405 interim AV verdict using McAfee VIRAL
Wed Sep 13 11:42:38 2017 Info: MID 405 antivirus positive 'EICAR test file'
Wed Sep 13 11:42:38 2017 Info: MID 405 enqueued for transfer to centralized quarantine "Virus" (a/v verdict VIRAL)
Wed Sep 13 11:42:38 2017 Info: MID 405 queued for delivery
Wed Sep 13 11:42:38 2017 Info: New SMTP DCID 239 interface 10.1.2.84 address 10.1.2.87 port 7025
Wed Sep 13 11:42:38 2017 Info: DCID 239 TLS success protocol TLSv1.2 cipher DHE-RSA-AES256-GCM-SHA384 the.cpq.host
Wed Sep 13 11:42:38 2017 Info: Delivery start DCID 239 MID 405 to RID [0] to Centralized Policy Quarantine
Wed Sep 13 11:42:38 2017 Info: Message done DCID 239 MID 405 to RID [0] (centralized policy quarantine)
Wed Sep 13 11:42:38 2017 Info: MID 405 RID [0] Response 'ok: Message 49 accepted'
Wed Sep 13 11:42:38 2017 Info: Message finished MID 405 done
Wed Sep 13 11:42:43 2017 Info: DCID 239 close
```

Die gleiche Nachricht, die von Sophos gesendet und gescannt wird:

```
Wed Sep 13 11:44:24 2017 Info: New SMTP ICID 307 interface Management (10.1.2.84) address 10.1.2.85 reverse dns host zane.local verified yes
```

Wed Sep 13 11:44:24 2017 Info: ICID 307 ACCEPT SG UNKNOWNLIST match sbrs[none] SBRS None country Australia
Wed Sep 13 11:44:24 2017 Info: Start MID 406 ICID 307
Wed Sep 13 11:44:24 2017 Info: MID 406 ICID 307 From: <joe@example.com>
Wed Sep 13 11:44:24 2017 Info: MID 406 ICID 307 RID 0 To: <bob@av.esa>
Wed Sep 13 11:44:24 2017 Info: MID 406 Message-ID '<20170913153946.E20C7A0121@example.com>'
Wed Sep 13 11:44:24 2017 Info: MID 406 Subject 'A/V test attachment'
Wed Sep 13 11:44:24 2017 Info: MID 406 ready 1057 bytes from <joe@example.com>
Wed Sep 13 11:44:24 2017 Info: MID 406 attachment 'av.txt'
Wed Sep 13 11:44:24 2017 Info: ICID 307 close
Wed Sep 13 11:44:24 2017 Info: MID 406 matched all recipients for per-recipient policy my_av in the inbound table
Wed Sep 13 11:44:24 2017 Info: MID 406 interim AV verdict using Sophos VIRAL
Wed Sep 13 11:44:24 2017 Info: MID 406 antivirus positive 'EICAR-AV-Test'
Wed Sep 13 11:44:24 2017 Info: MID 406 enqueued for transfer to centralized quarantine "Virus" (a/v verdict VIRAL)
Wed Sep 13 11:44:24 2017 Info: MID 406 queued for delivery
Wed Sep 13 11:44:24 2017 Info: New SMTP DCID 240 interface 10.1.2.84 address 10.1.2.87 port 7025
Wed Sep 13 11:44:24 2017 Info: DCID 240 TLS success protocol TLSv1.2 cipher DHE-RSA-AES256-GCM-SHA384 the.cpq.host
Wed Sep 13 11:44:24 2017 Info: Delivery start DCID 240 MID 406 to RID [0] to Centralized Policy Quarantine
Wed Sep 13 11:44:24 2017 Info: Message done DCID 240 MID 406 to RID [0] (centralized policy quarantine)
Wed Sep 13 11:44:24 2017 Info: MID 406 RID [0] Response 'ok: Message 50 accepted'
Wed Sep 13 11:44:24 2017 Info: Message finished MID 406 done
Wed Sep 13 11:44:29 2017 Info: DCID 240 close

In dieser Übung ESA wird "Virus Infected Messages" (Virusinfizierte Nachrichten) für "Action Applied to Message" (Auf Nachricht angewendete Aktion) in die Quarantäne für die jeweilige E-Mail-Richtlinie konfiguriert. Die Aktion für Ihre ESA kann variieren, abhängig von der Aktion, die für mit Viren infizierte Nachrichten durchgeführt wird, die von Antivirus-Programmen in Ihrer Mail-Richtlinie behandelt werden.

Zugehörige Informationen

- [Technischer Support und Dokumentation - Cisco Systems](#)